

A YANG Data Model for Network Incident Management

draft-ietf-nmop-network-incident-yang-03

Authors:

Tong Hu(hutong@cmhi.chinamobile.com)

Luis Contreras (luismiguel.contrerasmurillo@telefonica.com)

Qin Wu(bill.wu@huawei.com)

Nigel Davis (ndavis@ciena.com)

Chong Feng(Fengchonglly@gmail.com)

Contributors:

[Thomas Graf \(thomas.graf@swisscom.com\)](mailto:thomas.graf@swisscom.com)

Zhengqiang Li (li_zhenqiang@hotmail.com)

Yanlei Zheng (zhengyanlei@chinaunicom.cn)

Yunbin Xu (xuyunbin@caict.ac.cn)

Xing Zhao (zhaoxing@caict.ac.cn)

Chaode Yu(yuchaode@huawei.com)

Update since Last IETF meeting

- WG Github:

<https://github.com/ietf-wg-nmop/draft-ietf-nmop-network-incident-yang/issues>

- Draft Update (#22,#23,#26)

- Cross-check terminologies across NMOP drafts based on Adrian's comments.
 - Two new terminologies are added
 - Reuse terminologies in the terminology draft as much as possible
- Align with the Terminology draft based on Thomas's comments.
- Clarify the relation between the Network Incident, and Customer Incident.
- Clarify the relation between fault, problem, incident, service.

- Model Update

- None.

- Authors and Contributors list refresh
- Update Appendix with some descriptive text for example
- Other Editorial Changes for consistency

Align Terminologies with draft-ietf-nmop-terminology

Reuse Terminologies in [I-D.ietf-nmop-terminology]

- * alarm
- * resource
- * event
- * problem
- * incident
- * anomaly
- * cause

Introduce two new Terminologies

Service impact analysis: A process that uses machine learning to evaluate whether the network service has been impacted by the network incident and map network incident to one or a set of network service, which can reduce massive fault/alarms reporting, speed up troubleshooting, and assure network service performance and availability.

Root cause: A factor is considered the root cause of a problem if removing it prevents the problem from recurring. Conversely, a causal factor is a contributing action that affects an incident/ event's outcome but is not the root cause.

Align Terminologies with draft-ietf-nmop-terminology

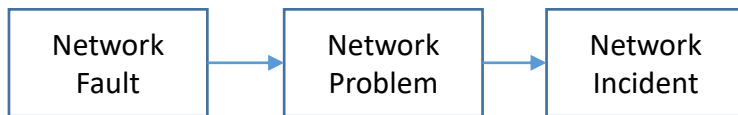
Update 'Incident Management' term

Incident management: Lifecycle management of network incidents, including network incident identification, reporting, acknowledgement, diagnosis, and resolution. Different from the traditional fault management, it take various different data sources including alarms, metrics, and other anomaly information and aggregate them into one or a few amount of network incidents irrespective of layer through correlation analysis and the service impact analysis. One fault on the network device can cause multiple network incidents, e.g., multiple service offerings that are dependent on that device will go down and others may suffer increased latency as redundant routes become more congested. A network incident might impact one or a set of network services. The network incident can also been seen as customer incident [TMF724A] when service SLA associated with one specific network service and network incident has been affected. How customer incident is translated from the network incident is beyond scope of this document.

Discussion of relation between fault, problem and incident

- This comment was raised by Brad during incident yang draft review by Thomas

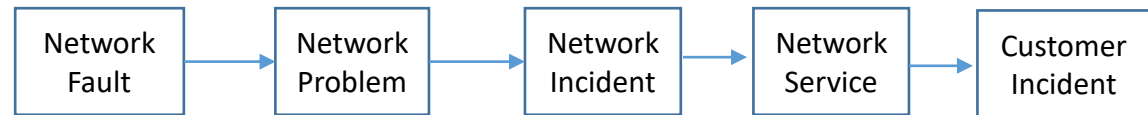
Option 1: Focus on Network Level



See section 3.2 Incident and problem definition of draft-ietf-nmop-terminology :

1. The fact of that unexplained recent Fault is a Problem.
2. An Incident results from one or more Problems, and a Problem may give rise to or contribute to one or more Incidents.

Option 2: Distinct Network Incident from Customer Incident



Brad Peter:

1. Customer Incidents and Network Incidents can be different entities
2. ITIL focus is on Customer Incidents and restoring customer services.
3. Network Incident creates a list of Impacted Network Services, Customer Incidents may or may not be in the list of Impacted Network Services.

Thomas:

1. A customer incident usually contains a relationship to the SLA while the network incident to the SLO.
2. The network problem relates to SLI where operational metrics are being considered.

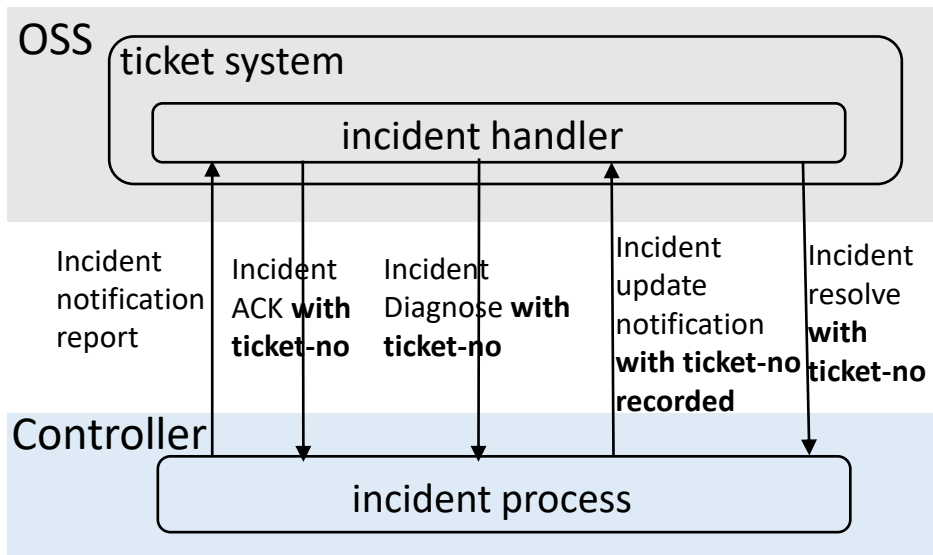
Resolution:

Clarify the relation between network incident and customer incident in both Introduction and Incident management definition.

Open Discussion: correlation with trouble tickets

One of the objectives of incident management is to identify root causes and reduce duplicated ticket amounts.

Question: Should we manage the correlation between network incidents and trouble tickets in the YANG data model?



```

notifications:
  +---n incident-notification
    +--ro incident-no?  incident-ref
    +---...
rpcs:
  +---x incident-acknowledge
  | +---w input
  | +---w incident-no*  incident-ref
  +---x incident-diagnose
  | +---w input
  | | +---w incident-no*  incident-ref
  +---x incident-resolve
  +---w input
  +---w incident-no*  incident-ref
  
```



```

notifications:
  +---n incident-notification
    +--ro incident-no?  incident-ref
    +--ro ticket-no?  string
    +---...
rpcs:
  +---x incident-acknowledge
  | +---w input
  | +---w incident-no*  incident-ref
  | +---w ticket-no?  string
  +---x incident-diagnose
  | +---w input
  | | +---w incident-no*  incident-ref
  | | +---w ticket-no?  string
  | +--ro output
  | +--ro task-id?  string
  +---x incident-resolve
  +---w input
  +---w incident-no*  incident-ref
  +---w ticket-no?  string
  
```

Open Discussion: incident diagnosis task list

The current document defines an incident-diagnosis RPC to identify root causes; and an incident update notification is triggered to report the diagnosis status if successful.

Question: Should we also define an incident-diagnosis-task list to report the following:

- The current status (e.g., created, diagnosing, diagnosed, finished) of each diagnosis task
- Task start time, end time, diagnosis result (succeeded, failed), failure description, etc.
- root causes, root events, repair recommendations, etc.

```
+---x incident-diagnose
| +---w input
| | +---w incident-no*  incident-ref
```



```
+---x incident-diagnose
| +---w input
| | +---w incident-no*  incident-ref
| | +---w ticket-no?  string
| +--ro output
| +--ro task-id?  string
```

```
+--ro incident-diagnosis-tasks
+--ro incident-diagnosis-task* [task-id]
+--ro task-id?      String
+--ro incident-no*   incident-ref
+--ro ticket-no?   string
+--ro start-time?   yang:date-and-time
+--ro end-time?     yang:date-and-time
+--ro task-state?   enumeration
+--ro diagnosis-result?  enumeration
+--ro diagnosis-result-description? String
+--ro root-causes
...
+--ro root-events
...
+-- ro repair-advice
```

Open Discussion: Service Impact Analysis

The current document only provides service impact analysis definition, but doesn't provide details on how service impact analysis works with network monitoring to get all necessary data. Here is one example of relevant data collection.

Supported Resources and Corresponding PM Capabilities

- Resource-type: network element, interface, board, termination point, tunnel termination point
- Indicator-name: defined as "String" type, compatible for extension, example:
Network element: CPU usage, memory usage, etc.
Interface: Ingress unicast packets, Ingress discard packets. Ingress error packets, etc.

TCA Management

- profile: pre-define the TCA configurations for specified indicators
 - Threshold-type: upperbound-trigger, upperbound-clear, lowerbound-trigger, lowerbound-clear
 - Severity: indicate the alarm severity once the threshold is triggered, i.e., critical, major, minor, warning
- Tca: apply profile or define TCA configuration directly for resources

Monitor task

- period: the period to collect the performance data
- Admin status: enable/disable

```
module: ietf-resource-pm
+--rw performance-monitoring
  |--rw resources
  | +--rw resource-list* [resource]
  |   +--rw resource          union
  |   +--ro resource-type?    identityref
  |   +--ro holding-time?     uint8
  |   +--ro indicator-name*   string
  |   +--ro sub-resources*    -> ../resource
  |
  |--rw tca-management
  | +--rw profiles
  | | +--rw profile* [profile-id]
  | | | +--rw profile-id      yang:uuid
  | | | +--rw profile-name?   string
  | | | +--rw tca-cfg
  | | | | +--rw tca-indicator* [indicator-name threshold-type per
  | | | | | +--rw indicator-name      string
  | | | | | +--rw indicator-value     string
  | | | | | +--rw indicator-value-unit string
  | | | | | +--rw threshold-type     enumeration
  | | | | | +--rw period             identityref
  | | | | | +--rw severity           identityref
  | | |
  | | | +--rw tcas
  | | | | +--rw tca* [resource]
  | | | | | +--rw resource          -> /performance-monitoring/resou
  | | | | | +--ro resource-type?    identityref
  | | | | | +--ro admin-status?     enumeration
  | | | | | +--rw applied-profiles
  | | | | | | +--rw profile* [profile-id]
  | | | | | | | +--rw profile-id    -> ../../../../profiles/profi
  | | | | | +--rw tca-cfg
  | | | | | | +--rw tca-indicator* [indicator-name threshold-type per
  | | | | | | | +--rw indicator-name      string
  | | | | | | | +--rw indicator-value     string
  | | | | | | | +--rw indicator-value-unit string
  | | | | | | | +--rw threshold-type     enumeration
  | | | | | | | +--rw period             identityref
  | | | | | | | +--rw severity           identityref
  | | |
  | | | +--rw monitor-tasks
  | | | | +--rw monitor-task* [task-id]
  | | | | | +--rw task-id          yang:uuid
  | | | | | +--rw resource?       -> /performance-monitoring/resources/r
  | | | | | +--ro resource-type?   identityref
  | | | | | +--rw task-name?      string
  | | | | | +--ro admin-status?    enumeration
  | | | | | +--ro task-status?     enumeration
  | | | | | +--rw task-cfg
  | | | | | | +--rw period?        identityref
  | | | | | | +--rw indicators
  | | | | | | |
  | | | | | | | +--rw indicator* [indicator-name]
  | | | | | | | | +--rw indicator-name      string
  | | | | | | | | +--rw indicator-value-unit? string
```

Question: Should this be documented in this draft?

Next Step

- 4 more issue tickets have been closed in the github
 - <https://github.com/ietf-wg-nmop/draft-ietf-nmop-network-incident-yang/issues>
- Additional comments and suggestions are welcome
- Continue to improve the draft based on input and comments!